The Information Commissioner's response to the Digital Competition Expert Panel's independent review consultation on 'The State of Competition in the Digital Economy'

1. The Information Commissioner has responsibility for promoting and enforcing the EU General Data Protection Regulation (GDPR), the Data Protection Act 2018 ("DPA"), the Freedom of Information Act 2000 ("FOIA"), the Environmental Information Regulations 2004 ("EIR") and the Privacy and Electronic Communications Regulations 2003 ("PECR"). She is independent from government and upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The Commissioner does this by providing guidance to individuals and organisations, solving problems where she can, and taking appropriate action where the law is broken.

2. The GDPR and the DPA are new laws which took effect from May 2018, replacing the Data Protection Act 1998. They build on existing data protection rights, such as the right to access, and introduce new ones, for example, the right to data portability.

3. The Commissioner's fundamental objective during her term is to build a culture of data confidence in the UK, helping our digital economy to grow in a strong and sustainable way. In order to achieve this objective it is essential that government builds privacy into the development of public policy, ensuring that individuals' fundamental privacy rights are central to legislative and regulatory decisions. The Commissioner believes that, where policy proposals include the processing of personal data, there should not be a choice between privacy *or* innovation, but a focus on privacy *and* innovation.

4. The Information Commissioner welcomes the opportunity to respond to the Digital Competition Expert Panel's independent review consultation on 'The State of Competition in the Digital Economy'.

5. This response focuses on digital market competition issues that raise data protection considerations. These include:

    - Innovation and privacy by design and default;
    - Data Portability and interoperability;

- Artificial Intelligence (AI), machine learning and algorithmic transparency;
- Data Trusts;
- Certification Schemes;
- Codes of Conduct.

Privacy and Competition

6. Of the G20 countries the digital economy in the UK is the highest proportion of GDP, and this could grow by another third in the medium term. This provides enormous opportunities for business seeking to expand in the data driven economy.

7. The introduction of the GDPR on 25th May this year, brought a series of new requirements and responsibilities upon businesses in how they approached data handling and data protection. Attention is being increasingly focussed upon the opportunities data protection presents. One of the overlooked aspects of this opportunity is the facilitation and promotion of competition and innovation through data protection. This response hopes to outline what the opportunities are and more importantly how they can have positive impacts upon businesses and market places.

8. One of the difficulties in the area where data meets business is that the greater the proportion of personal data a company possesses the more likely it is to accumulate more. Data has a natural propensity toward aggregation. This creates a challenge around the creation of monopolies, an issue that has become increasing prominent in recent years with the emergence of extremely large internet based corporations. For policy makers the challenge is to facilitate competition, while convincing businesses already in a strong position that data protection is a catalyst to innovation, rather than an impediment.

9. This response will enumerate a series of concepts that spring from the GDPR and DPA 2018 and detail their immediate and potential impacts. But there a series of principles that underpin the legislation and how it interacts with competition policy. The concepts of transparency, accountability and trust are central to data protection in and of itself, but furthermore are the basis for how competition can flourish in the digital world. As more and more commerce and other business moves online, demand from users of these services for greater protections has grown.

10. In order for individuals, as consumers, to have confidence in digital businesses they must have trust that their personal data will be handled responsibility and in ways that they have agreed.

Transparency is the first cornerstone of this. The GDPR allows people to understand in much clearer terms what data companies possess and how it is being processed – through tools such as subject access requests, algorithmic transparency, consent and other lawful bases for processing. The second cornerstone is around accountability, and the faith that if data is misused there are remedies for individuals and consequences for those who breach the law.

11. The specific areas, outlined in this submission, which put these principles into practice are all in part aimed at fostering the trust and confidence that enables competition, which allows customers to move their data with confidence, to undertake transactions, and that encourages businesses to innovate in order to retain customers.

Innovation and Privacy by Design and Default

12. In many instances data concentration is seen as advantageous by large corporations that already possess large amounts of data. Intellectual Property laws often underpins this. In much the same way, Data Protection laws should also be ingrained across the spectrum of economic development to help encourage competition and innovation. Central to this is the principle of data protection by design and default.

13. Privacy by design has two major advantages in terms of bolstering competitiveness. Firstly, it mitigates what could be described as "regulatory burden" by building in protection of personal data from the very conception of businesses, projects or functions. Secondly, it guards against potential breaches by 'hard-wiring' systems for fair and secure processing into any handling of data, preventing loss of trust in a given business, and avoiding censure from regulators.

14. There are broad competitive advantages to good privacy practices, such as privacy by design and default, revolving around basic concepts like customer satisfaction. Equally, an enterprise which is built upon sound data protection principles will find itself unburdened by out-of-date customer information, duplicated data, wasted storage, and redundant man hours spend meeting data protection requirements retrospectively. The concepts of data minimisation and purpose limitation allow companies to become streamlined and nimble in their use of data, opening up avenues to competitive advantage.

15. Advances in technology should not mean organisations racing ahead of people's rights. Innovation relies on consumer trust and therefore the digital economy depends on the trust of consumers to engage with it. Organisations need to understand that, unless they are

trusted to properly look after people's personal data, they will fail to realise its potential benefits to their business or the wider economy.

16. The GDPR requires that appropriate technical and organisational measures are put in place to implement the data protection principles and safeguard individual rights. This is 'data protection by design and by default'. This means that data protection must be 'baked' into processing activities and business practices, from the design stage right through the lifecycle of a project to its completion.

Data Portability and Interoperability

17. As GDPR beds in, business will increasing turn its attention toward the opportunities it presents, in addition to simply complying with its requirements. Data portability and interoperability, as a potential competitive advantage, could be one of these opportunities.

18. The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without affecting its usability.

19. The role of data portability as a catalyst to greater competition is clear. By bolstering the right of individuals to move their data from one business or platform to another creates incentives in the marketplace for better services, better products, and greater innovation.

20. Data portability creates a more level playing field between large corporations who enjoy greater degrees of data concentration and smaller enterprises who will be able to attract customers unhindered by cumbersome processes for engaging their data. Individuals will feel less tethered to a company which hold their data.

21. Interoperability is a related advantage for competition. By requiring that data processed by a given company is held, developed and made transferable in a way that other businesses can use, it makes it simpler for individuals to move their personal data; once again bolstering the need for enterprise to develop good services and innovate to retain or attract customers.

22. Doing this will enable individuals to take advantage of applications and services that use this data to find them a better deal or help them understand their spending habits.

23. There are a number of different components that need to be in place for data portability to work. Organisations are going to need to consider what the building blocks are to achieve this. Big tech has already launched schemes looking into this and solutions are inevitable.

24. There are, of course, data protection risks related to this GDPR requirement, such as the risk of 'data leakage' occurring during a transfer of data. Organisations will need to consider this and take precautions to mitigate against the risks. Too many leaks are likely to lead to the eroding of consumer trust and engagement with the market.

Artificial Intelligence, Machine Learning and Algorithmic Transparency

25. The implications of the use of Artificial Intelligence (AI) and machine learning in competition could be extensive in terms of consumer rights. Competition policy should take into account how such technology can affect the equality and fairness with which consumers are treated in the digital markets.

26. AI is a type of automated processing that has its own unique risks. AI programs often include machine-learning and do not linearly analyse data in the way they were originally programmed. Instead they learn from the data they have already analysed in order to respond intelligently to new data and adapt their outputs accordingly.

27. This brings the possibility of AI-enabled technology making significant decisions about people, with little or no human oversight. There is also the very real risk that biases are introduced into AI either from the development of a product or through the way in which it develops as part of the machine learning process.

28. People have developed a mistrust in the use of AI technology. This is likely to affect competition in this area unless organisations can increase consumer trust.

29. Artificial Intelligence, machine learning and the use of algorithms present an enormous range of opportunities for businesses. The speed of processing, decision-making and exponential learning can improve services, allow many more transactions, and free up manpower. However, these opportunities can only be utilised and maximised if the risks around privacy and data processing are adequately addressed.

30. Take for example algorithms. Individuals using digital services or businesses are likely to appreciate greater speed of processing but only if there is a sufficient degree of transparency as do how the algorithms work and how decisions about them are made using their own personal data. An absence of this will create a reluctance to engage.

31. Algorithmic transparency can also encourage innovation and competition by allowing businesses to learn from each other, develop best practice, and prevent oversensitive protection of algorithms by large corporations seeking to retain monopolistic market share.

32. Bias in AI can encourage the perpetuation of poor service, or limited options for some consumers which is anathematic to competition. By contrast fair and open AI practices will do the opposite and encourage opportunities for interaction between businesses and customers.

33. The GDPR has introduced a number of new requirements that could be used to mitigate against a lack of trust. Including a right for individuals to request human intervention or to challenge a decision.

34. Another key element that the GDPR introduces that could be used to resolve this issue is transparency. Providing individuals with information about how the AI works and the implications and likely outcomes from its use will increase understanding. That alongside regular reviews and data privacy impact assessments when making changes to systems or implementing new systems is likely to reduce breach risks and increase consumer trust.

Data Trusts

35. A “Data Trust” takes the concept of a legal trust and applies it to data. It provides a legal structure that allows for independent third-party stewardship of data. The idea behind data trusts is that they facilitate sharing between multiple organisations, but do so in a way that ensure that the proper privacy protections and other relevant protections are in place. There is a governance of the data, which ensures that the voices of interested parties are represented in that governance, and there is a fair sharing of the value that can be derived from those data. Data trusts have the potential to greatly increase the competitiveness of the digital markets.

36. Data trusts do not necessarily involve the processing of personal data. Those that don’t would be unlikely therefore to engage the requirements of the GDPR. Some data trusts use ‘anonymised’

personal data and where the data is truly anonymised the GDPR requirements would also not be engaged.

37. However, there are a number of considerations data trusts need to take into account. Those who use anonymised personal data need to ensure that they are not assuming the data they are using has anonymised where in reality it may be pseudonymised. The difference being that it is possible to re-identify pseudonymised data, resulting in the possible re-identification of the individual the data relates to. It should not be possible to re-identify truly anonymised data. The test in law is that if it is reasonably likely for re-identification to occur then the data is not truly anonymised.

38. Truly anonymised data is a more complex concept than might initially be thought. For example, data trusts will not only need to think about what is possible now in terms of re-identification but also what could be possible in the future. With open data sets a gamble is essentially being taken that future technology will not be developed that would enable the data to be re-identified. There are also risks around third-party access to that data and how they use it.

39. The issue is not soluble, having said that, organisations can address it by assessing the risks - including considering what third parties with access to the data might do with it – and taking reasonable precautions. The risks need not be a hindrance to the development of data trusts. They simply should be taken into account and the data trust developed with these considerations in mind – in other words privacy by design and default.

40. Data trusts encourage competition through innovation. They provide a mechanism for companies and businesses to try new things with data while taking steps to ensure that the privacy rights of individuals are protected. Likewise, ‘regulatory sandboxes’, like the one the ICO is establishing, encourage innovations by creating safe space for businesses to interact with real world customers helping them to develop approaches that utilise and are driven by sound data protection practices.

Certification Schemes

41. The concept of certification schemes in data protection was included in the GDPR. They are envisaged as a way to comply with the GDPR and enhance transparency. Certification is a way for organisations to demonstrate that their processing of personal data complies with the GDPR requirements in line with the accountability principle.

42. The ICO has no plans to accredit certification bodies or carry out certification at this time, although the GDPR does allow this.

43. The ICO will publish accreditation requirements for certification bodies to meet. The UK's national accreditation body (UKAS) will accredit certification bodies and maintain a public register of accredited certification bodies.

44. Signing up to a certification scheme is voluntary but could be considered a competitive advantage in the digital economy.

45. Certification is a mechanism for displaying trustworthiness to potential customers. Smaller businesses seeking to expand, or new companies with lesser brand recognition than established counterparts can demonstrate their willingness and ability to handle individuals' data in a way that is responsible and transparent, verified by a third party certification. This levels the playing field and fosters competition.

Codes of Conduct

46. Codes of Conduct were introduced by the GDPR as a way to help organisations to apply the GDPR effectively. They are expected to be sector specific and reflect the needs of different processing sectors and micro, small and medium sized enterprises. Trade associations or bodies representing a sector can create codes of conduct to help their sector comply with the GDPR in an efficient and cost effective way. They will have to submit them to the ICO for approval. Signing up to a code of conduct is also voluntary.

47. The ICO's role in codes of conduct will be to assess whether a monitoring body is independent and has expertise in the subject matter/sector. Approved bodies will monitor compliance with the code and help ensure that the code is appropriately robust and trustworthy.

48. Compliance with these Codes of Conduct with specific sectors will help not only help organisations to comply with the GDPR and demonstrate that compliance with the ICO but could also give them a competitive advantage over organisations who do not comply.

49. Codes of conduct can be a tool in fostering both competition and innovation. In the first instance, the sector specific guidance give confidence to businesses that they can/are handling data correctly. That confidence can be a springboard for innovation. Secondly, codes of practice are one strand of creating a level playing field for

businesses who process data, which is a prerequisite to encouraging competition.

Data Protection and Competition

50. It is too early to tell what the full extent of the impact of the GDPR on competition in the digital economy will be as organisations are currently mainly focused on basic compliance. However, as outlined above, it is likely to influence a number of areas in the markets development.

51. We note that the main considerations of this consultation are around concerns relating to the monopolization of the digital market, rather than data protection principles. However, the overlap between privacy and competition is much more real now than a few years ago. The competitive advantages organisations might gain through compliance with the GDPR should be considered when deciding competition policy.

52. As laid out here, organisations themselves can improve their competitive edge in the digital market by engaging and complying with data protection principles, seeing them as an opportunity rather than a burden. The key theme underpinning this opportunity is viewing it as privacy *and* innovation, rather than privacy *or* innovation.